IN THE U.S. DISTRICT COURT FOR THE MIDDLE DISTRICT OF TENNESSEE

TRAVELERS CASUALTY AND SURETY COMPANY OF AMERICA	)	
Plaintiff,	)	
v.	)	**No. _____**
	)	**(Jury Demand)**
CHANGE HEALTHCARE, INC., UNITEDHEALTH GROUP, INC., and OPTUM, INC.	)	
Defendants.	)	

COMPLAINT

Plaintiff Travelers Casualty and Surety Company of America ("Travelers"), as subrogee and assignee of J&B Medical Supply Company, Inc. ("J&B") by and through counsel, states the following for its Complaint against Defendants Change Healthcare, Inc. ("Change"), UnitedHealth Group, Inc. ("UnitedHealth"), and Optum, Inc. ("Optum") (collectively "Defendants").

PARTIES

1. Travelers is a corporation organized and existing under the laws of the State of Connecticut with its principal place of business in Hartford, Connecticut. Travelers is a citizen of the State of Connecticut for purposes of diversity jurisdiction under 28 U.S.C. § 1332(a).

2. Change is a corporation organized and existing under the laws of the state of Delaware with its principal place of business in Nashville, Tennessee. Change is a citizen of the State of Tennessee for purposes of diversity jurisdiction under 28 U.S.C. § 1332(a).

3. UnitedHealth is a Delaware corporation with its principal place of business in

Minnetonka, Minnesota. UnitedHealth Group operates and maintains several offices in Tennessee, including in Brentwood, Lenoir City, Kingston, Maryville, Columbia, Cordova, Smyrna, Gallatin, and Nashville. UnitedHealth owns Change and Optum.

4. Optum is a Delaware Corporation with its principal place of business in Eden Prairie, Minnesota. Optum is a subsidiary of UnitedHealth, and Change is a part of Optum.

JURISDICTION AND VENUE

5. This Honorable Court possess subject matter jurisdiction over this Complaint pursuant to 28 U.S.C. § 1332(a) because the matter in controversy exceeds the sum or value of $75,000.00, exclusive of interest and costs, and the matter in controversy is between citizens of different states.

6. Venue is proper in the United States District Court for the Middle District of Tennessee pursuant to 28 U.S.C. § 1391, because the Change is a resident of the State of Tennessee and resides in the Middle District of Tennessee.

FACTUAL ALLEGATIONS

A. Travelers Is the Subrogee and Assignee of J&B

7. Travelers is an insurance company that provides insurance coverage to (among others) services health care providers and businesses in the medical industry.

8. Travelers issued Wrap+ CyberRisk Policy No. 107847335 (the "Policy") on behalf of its insured, J&B, a medical supplier, based in Wixom, Michigan.

9. Travelers is the subrogee and successor to the interests of J&B regarding the events described herein by virtue of subrogation and assignment, as discussed below.

10. The Policy provides a coverage limit of $5,000,000 for Computer Legal Experts and Privacy Notification expenses, subject to $50,000 retention. The Policy also provides for

$5,000,000 in Dependent Business Interruption. The Policy's aggregate limit is $5,000,000.

11. J&B is a medical supply provider based in Wixom, Michigan. It has approximately 600 employees and 200 subcontractors.

12. J&B contracted with Change for its Assurance Plus Subscription, Assurance Plus Paper Claim, Assurance Plus HCDirect Original, and Acuity Revenue Cycle Analytics Assurance Module services (the "Change Services"). Such services are a necessary part of J&B's day-to-day operations.

13. On February 21, 2024, J&B encountered a major disruption to its operations when it was unable to access features, services, and processes provided as part of the Change Services.

B. The Change Data Breach

14. UnitedHealth is the largest healthcare insurer in the United States, and the fifth largest company in the United States. UnitedHealth reaches 152 million individuals across all facets of its business, from insurance to physical practice, to home health, and pharmacy. In 2023 alone, UnitedHealth generated $324 billion in revenue.

15. Optum is a healthcare service provider with business interests encompassing technology and related services, pharmacy care services, and various direct healthcare benefits. Optum has been a subsidiary of UnitedHealth since 2011. After Change was purchased by UnitedHealth, Change became a part of Optum.

16. Change is a Tennessee based healthcare company that provides payment and revenue cycle services, clinical and imaging services, and other services to its clients. Change operates one of largest healthcare technology companies in the United States, processing 50% of medical claims in the United States for approximately 900,000 physicians, 33,000 pharmacies,

5,500 hospitals, and 600 laboratories.[1] Change processes 15 billion healthcare transactions a year and is involved in one of every three patient records.[2]

17. In order to provide these services, Change acquires, collects, and stores its client healthcare providers' patients' PII and PHI, which includes patient names, contact information, healthcare insurance information, medical records, dental records, payment records, and social security numbers.

18. Defendants are aware of its critical responsibility to safeguard this sensitive information and the need to implement effective cyber security measures to prevent the information's theft. Defendants thus assumed equitable and legal duties to safeguard and keep patients' PII and PHI confidential and use the information purely for business purposes.

19. Change acknowledged and understood its duties and responsibilities, promising that "Change Healthcare is committed to the privacy and security of healthcare data and meets or exceeds HIPAA Privacy and Security Rule requirements."[3]

20. Despite the imposition of these duties, Defendants failed to implement reasonable data security measures to protect patient information and its computer systems and services upon which J&B relied.

21. On February 21, 2024, Defendants failed to prevent a cyberattack perpetrated by the ransomware group "ALPHV/BlackCat" affecting a number of their systems and services. The cyberattack infiltrated Defendants' inadequately protected network and accessed highly sensitive

---

[1] *US health departments open probe into UnitedHealth hack*, Reuters (Mar. 13, 2024) https://www.reuters.com/technology/cybersecurity/hhs-opens-probe-into-hack-unitedhealth-unit-2024-03-13/ (last accessed June 28, 2024).
[2] *Letter to Health Care Leaders on Cyberattack on Change Healthcare*, U.S. Department of Health and Human Services (Mar. 10, 2024), https://www.hhs.gov/about/news/2024/03/10/letter-to-health-care-leaders-on-cyberattack-on-change-healthcare.html (last accessed June 28, 2024).
[3] *Privacy And Security*, Change Healthcare, https://support.changehealthcare.com/customer-resources/hipaa-simplified/privacy-security ((last accessed June 28, 2024).

information which was unprotected (the "Data Breach").

22. Ransomware attacks encrypt a target's computer systems in a manner that prevents the target from gaining access to their material, unless a ransom is paid in return for the passcode required to decrypt the system. Such an attack is a common form of cyberattack, one that Defendants should have anticipated it would be threatened with, especially due to the types of valuable information in its possession.

23. The ransomware group was in the company's networks for more than a week before they launched the ransomware attack.[4]

24. Andrew Witty, the CEO of UnitedHealth, stated that the Change cyberattack, which disrupted healthcare systems nationwide, started when hackers entered a server that lacked a basic form of security: multi-factor authentication.[5]

25. Multi-factor authentication is a simple security measure that can be implemented in a matter of days or weeks, as is demonstrated by the speed at which Defendants implemented multi-factor authentication after discovering the Data Breach.

26. In response to the Data Breach, Defendants pulled the suspended operations and use of all of their online systems to prevent further impact rather than keep unaffected systems operational. As a result of Defendants' choice to disconnect its systems, J&B was unable to access or utilize any of the Change Services, including benefits verification, claims submissions, and

[4] James Rundle, *Hackers Broke Into Change Healthcare's Systems Days Before Cyberattack*, Wallstreet Journal (April 22, 2024) https://www.wsj.com/articles/change-healthcare-hackers-broke-in-nine-days-before-ransomware-attack-7119fdc6 (last accessed July 16, 2024) ("Between Feb. 12 and when the ransomware was detonated on Feb. 21, the hackers were moving laterally within Change's network … The length of time the attackers were in the network suggests they might have been able to steal significant amounts of data from Change's systems.").

[5] *Change Healthcare cyberattack was due to a lack of multifactor authentication, UnitedHealth CEO says*, Associated Press News (May 1, 2024) https://apnews.com/article/change-healthcare-cyberattack-unitedhealth-senate-9e2fff70ce4f93566043210bdd347a1f (last accessed June 28, 2024).

prior authorizations. Without these crucial systems, J&B was barred from receiving any compensation for its services to patients and further prevented J&B from providing goods and services to its customers thereby permanently depriving J&B from the ability to realize revenue and causing other harm to J&B. The systems remained disconnected throughout most of March causing major disruptions to J&B's business operation and preventing J&B from making millions of dollars of sales and realizing the profit off of those lost sales.

27. Defendants did not inform J&B of the cyberattack until after J&B lost access to Change's services.

28. On or around March 1, 2024, Defendants tendered a $22,000,000 ransom payment to the threat actors in exchange for a decryption key and promise to delete sensitive data.

29. J&B reported the incident to Travelers on March 1, 2024.

30. As a result of the disruption, J&B's operations were crippled starting on February 21, 2024. J&B had thousands of orders for which it could not confirm insurance eligibility, and as a result, could not process or ship orders for prescriptions and medical equipment. J&B's cash collections came to a halt as millions of dollars owed to it could not be transmitted through Change's systems. As a Tier-1 Provider, J&B's customers did not have alternative means of obtaining prescriptions and medical equipment.

31. J&B and its internal IT group worked around the clock to isolate workarounds and applied for financial relief through Optum's Temporary Funding Assistance Program.

32. The disruption to J&B's business was the direct result of Defendants' failure to implement and follow basic data security procedures, *inter alia*, multi-factor authentication.

33. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data an as unfair act or practice

prohibited by Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45.

34. Defendants were also covered by HIPAA (*see* 54 C.F.R. § 160.102) and are therefore required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information").

35. Although the Defendants' businesses involve the handling of highly sensitive data, Defendants implemented inadequate data security practices that they knew or should have known put their client and their client's customers at risk of having their PII and PHI exposed, especially as a leading healthcare technology company and purported expert in the field. Defendants knew or should have known that any cyberattacks meant to obtain PII and PHI would also lead to disruptions of services they offered to J&B.

36. On March 4, 2024, J&B provided a notarized proof of loss claiming in excess of $5,000,000 as a result of the disruption.

37. On March 4, 2024, J&B submitted to Travelers a notarized proof of loss claiming a loss in excess of $5,000,000 as a result of the disruption. Travelers reviewed the claim, determined coverage was available and made payment to J&B under the Policy.

CLAIMS FOR RELIEF
COUNT I – NEGLIGENCE
(Against All Defendants)

38. Travelers hereby restates the averments contained in the foregoing paragraphs of this complaint as if fully set forth herein.

39. At all times herein relevant, Defendants owed J&B a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their computer systems and networks.

40. These systems, *inter alia*, included claims processing, revenue cycle services, payment processing services, of which Defendants owed J&B a duty to act with reasonable care to safeguard so that claims and revenue would be processed on time and for the correct amounts.

41. Defendants owed a duty of care to not subject J&B to an unreasonable risk of harm because J&B was the foreseeable and probable victim of any inadequate security practices.

42. Defendants owed J&B a duty of reasonable care to preserve and protect the information being stored, transferred, and secured and to ensure that Change's payment processing and other services stayed operational and did not experience extended outages or unavailability.

43. This duty included, *inter alia*, maintaining and testing Change's security systems and computer networks, implementing training and other protocols and procedures to guard against cyberattacks, and taking other reasonable security measures to safeguard and adequately secure its systems form unauthorized access and use.

44. Defendants knew or should have known of the vulnerabilities of their data security systems and the importance of adequate security. Defendants knew or should have known about numerous well-publicized data breaches.

45. Defendants knew or should have known that its data systems and networks did not adequately safeguard the claims processing and revenue cycle services.

46. Because Defendants knew that any breach to its system could result in damage to numerous customers, including J&B, Change had a duty to adequately protect its data systems.

47. Defendants breached their duty to J&B by failing to provide fair, reasonable, or

adequate computer systems and data security practices to safeguard the services they provided to J&B.

48. Defendants consistently ignored standards encompassed in the NSIT Cybersecurity Framework Version 1.1 and CIS CSC, which are accepted industry standards.

49. J&B's willingness to entrust Defendants with its processing needs was predicated on the understanding that Defendants take adequate security precautions.

50. As Defendants' systems also collected patient PII and PHI, Defendants also had independent duties under federal and state law to ensure that their systems were secure and to promptly notify customers, like J&B, of the Data Breach.

51. Defendants' willful failure to abide by its duties was wrongful, reckless, and/or grossly negligent in light of the foreseeable risks and known threats.

52. As a proximate and foreseeable result of Defendants' grossly negligent conduct, J&B has suffered damages and is at imminent risk of additional harm and damages.

53. Additionally, the law imposes an affirmative duty on Defendants to timely disclose the unauthorized access as well as their intention to completely shut down their systems, which, *inter alia*, resulted in J&B's inability to process claim correctly and/or timely.

54. Defendants breached their duty to notify J&B of the unauthorized access by waiting an unreasonably long period of time after learning of the Data Breach to notify J&B and then by failing to provide J&B with sufficient information regarding the breach.

55. Further, through their failure to provide timely and clear notification of the Data Breach to J&B, Defendants prevented J&B from taking meaningful, proactive steps to secure

processing needs which caused injury to J&B.

56. There is a close causal connection between Defendants' failure to implement security measures to protect J&B's processing requirements.

57. Defendants' wrongful actions, inactions and omissions constituted and continue to constitute common law negligence.

58. The damages J&B has suffered, as alleged above, and will continue to suffer, were and are the direct and proximate result of Defendants' grossly negligent conduct.

59. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair [...] practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII like the processing of confidential claims.

60. Furthermore, Defendants are HIPAA covered business associations that provide services to various healthcare providers. As a regular and necessary part of its business, Defendants collect and stores highly sensitive PHI of its clients' patients. Defendants have a duty under federal law to maintain the strictest confidentiality of the patient's PHI that they acquire, receive, and collect, and Defendants are further required to maintain sufficient safeguards to protect that PHI from being accessed by unauthorized third parties.

61. Defendants violated 15 U.S.C. § 45 and HIPAA by failing to use reasonable measures to protect PII and PHI like the processing of confidential claims and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI obtained and stored and

the foreseeable consequences of the immense damages that would result to J&B.

62. Defendants breached their duty to J&B by implementing unreasonable data security measures and by failing to keep data security as a top priority despite understanding and writing about the risk of data breached involving highly sensitive data and touting their own security capabilities.

63. Defendants were fully capable of preventing the Data Breach. Change, as sophisticated and experienced technology companies, knew of data security measures required or recommended by the FTC, and other data security experts which, if implemented, would have prevented the Data Breach from occurring at all, or limited the scope and depth of the Data Breach. Defendants thus failed to take reasonable measures to secure its system, creating vulnerability to a breach.

64. J&B is a consumer within the class of persons that 15 U.S.C. § 45 and HIPAA were intended to protect.

65. Moreover, the harm that has occurred is the type of harm that 15 U.S.C. § 45 and HIPAA were intended to guard against. The FTC has pursued many enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by J&B.

66. Defendants' violation of 15 U.S.C. § 45 and HIPAA constitutes negligence *per se*.

67. Defendants knew they were an attractive target for cyber criminals, particularly in light of data breaches experienced throughout the United States. The Data Breach was reasonably

foreseeable given the known high frequency of ransomware attacks and data breaches.

68. J&B was the foreseeable victim of Defendants' inadequate and ineffectual cybersecurity. The natural and probable consequences of Defendants' failure to adequately secure their information networks was a disruption in the services upon which Defendants knew that J&B and J&B's patients relied.

69. There is a close connection between Defendants' failure to employ reasonable security protections for its systems and the injuries suffered by J&B. Defendants' vulnerability to cyberattacks resulted in their system being taken down and the inability of J&B to access necessary services.

70. As a direct and proximate result of Defendants' negligence and negligence *per se*, J&B has suffered damages, including, *inter alia*, missed payments and out-of-pocket expenses associated with (i) disruption and interruption of its business and healthcare services to its patients, (ii) the failure to receive payments for the services rendered to its patients, (iii) costs associated with workarounds during the period that Change's services were down, (iv) notifying patients of the Data Breach, and (v) late penalties assessed for untimely payments of expenses. Further, J&B's damages include the time and effort spent finding workarounds during the period in which Change's systems were down and the time and effort spent researching and training on new healthcare payment software. The damages suffered by J&B continue and will result in other economic and non-economic losses.

71. Travelers has paid J&B's insurance claim based on Defendants' actions and now seek reimbursement for such actions. Travelers will have to pay additional insurance claims on behalf of other policyholders because of Defendants' actions.

COUNT II – BREACH OF CONTRACT
(Against Change Healthcare)

72. Travelers hereby restates the averments contained in the foregoing paragraphs of this complaint as if fully set forth herein.

73. Acting in the ordinary course of business, Change contracts with healthcare providers, like J&B, to provide its services. Its services allows Change to, *inter alia*, act as a middleman between healthcare providers and insurance companies. Healthcare providers submit insurance claims though the Change Platform, which Change sends to the insurance companies. After evaluation and processing, insurance companies then pay the healthcare providers.

74. J&B paid for Change's services.

75. In return for J&B's payment, Change promised that J&B would have access and be permitted to use its services.

76. In February 2024, following the Data Breach, Change disconnected its services – thereby severing J&B's access and use of the services and breaching its contractual obligations.

77. As a direct and proximate result of Change's breach, J&B sustained actual losses and damages. J&B alternatively seeks an award of nominal damages.

78. As a direct and proximate result of Change's breach, J&B sustained actual losses, lost profits, and damages in an amount to be proven at trial. J&B seeks an award of nominal damages in the alternative.

79. Change also breached certain terms in its contract regarding protection of PII acquired during the course of performance of the contract. These terms required Change to, *inter alia*, timely report data breaches to J&B, have adequate safeguards to protect PII, and to

implement technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PII.

80. Travelers has paid J&B's insurance claim based on Defendants' actions and now seek reimbursement for such actions. Travelers will have to pay additional insurance claims on behalf of other policyholders because of Defendants' actions.

COUNT III – BREACH OF IMPLIED CONTRACT
(Against All Defendants)

81. Travelers hereby restates the averments contained in the foregoing paragraphs of this complaint as if fully set forth herein.

82. Through each's course of conduct, Defendants and J&B entered into implied contracts for Defendants to implement data security adequate to safeguard and protect services, including claims processing and revenue cycle service materials, provided to J&B.

83. Defendants required J&B to provide and entrust J&B's claims processing and revenue cycle service materials as a condition of obtaining Change's services.

84. Defendants solicited and invited J&B to provide its claims processing and revenue cycle service materials as part of Defendants' regular business practices. J&B accepted Defendants' offer and provided its claims processing materials to Defendants.

85. J&B provided and entrusted its claims processing and revenue services materials to Defendants. In doing so, J&B entered into implied contracts with Defendants by which Defendants agreed to ensure that J&B's processing materials would not be defective or compromised.

86. A meeting of the minds occurred when J&B agreed to, and did, provide its claims

processing and revenue cycle services materials to Defendants, in exchange for, *inter alia*, the protection of its materials.

87. J&B fully performed its obligations under the implied contracts with Defendants.

88. Defendants' breaches caused economic and non-economic harm.

89. Travelers has paid J&B's insurance claim based on Defendants' actions and now seek reimbursement for such actions. Travelers will have to pay additional insurance claims on behalf of other policyholders because of Defendants' actions.

COUNT IV – BREACH OF CONFIDENCE
(Against All Defendants)

90. Travelers hereby restates the averments contained in the foregoing paragraphs of this complaint as if fully set forth herein.

91. During J&B's interactions with Defendants, Defendants were fully aware of the important and confidential nature of the processing materials that J&B provided them.

92. As alleged herein and above, Defendants' relationship with J&B was governed by promises and expectations that J&B's claims processing and revenue cycle service materials would be kept in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

93. Defendants provided their respective claims processing and revenue cycle services to J&B with the explicit and implicit understandings that Defendants would protect and not permit the materials to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

94. J&B also provided its claims processing and revenue cycle services materials to Defendants with the explicit and implicit understanding that Defendants would take precautions to protect those materials from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting its networks and data systems and ensuring that claim payments related to materials would be promptly paid and satisfied.

95. Due to Defendants' failure to prevent, detect, and avoid the Data Breach from occurring, *inter alia*, not following best information security practices to secure J&B's claim processing, J&B's materials were encumbered by and, not able to be used by J&B in the manner expected.

96. As a direct and proximate cause of Defendants' actions and/or omissions, J&B has suffered damages, as alleged herein.

97. But for Defendants' failure to maintain and protect J&B's claims processing and revenue cycle service materials in violation of the parties' understanding of confidence, its material would not have been accessed by, acquired by, and/or viewed by unauthorized third parties.

98. The injury and harm J&B suffered, and will continue to suffer, was the reasonably foreseeable result of Defendants' unauthorized misuse of J&B's materials. Defendants knew their data systems and protocols for accepting and securing J&B's materials had security and other vulnerabilities that placed J&B's materials in peril.

99. Travelers has paid J&B's insurance claim based on Defendants' actions and now seek reimbursement for such actions. Travelers will have to pay additional insurance claims on

behalf of other policyholders because of Defendants' actions.

COUNT V – BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(Against All Defendants)

100. Travelers hereby restates the averments contained in the foregoing paragraphs of this complaint as if fully set forth herein.

101. Every contract includes an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even if there is no breach of a contract's actual and/or express terms.

102. J&B has complied with and performed all conditions of its contracts with Defendants.

103. Defendants Breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices and to process claims and services in a timely and safe manner as a result of the Data Breach.

104. Defendants knew or should have known of the vulnerabilities of the systems that were exploited in the Data Breach.

105. Defendants acted in bad faith and/or with malicious motive in denying J&B the full benefit of its bargain as originally intended by the parties, thereby causing J&B damages in an amount to be determined at trial.

106. Travelers has paid J&B's insurance claim based on Defendants' actions and now seek reimbursement for such actions. Travelers will have to pay additional insurance claims on behalf of other policyholders because of Defendants' actions.

COUNT VI – BREACH OF FIDUCIARY DUTY
(Against All Defendants)

107. Travelers hereby restates the averments contained in the foregoing paragraphs of this complaint as if fully set forth herein.

108. In light of the special relationship between Defendants and J&B, whereby Defendants became the guardian of J&B's claim processing materials, Defendants became a fiduciary by their undertaking and guardianship of materials to act primarily for the benefit of J&B.

109. Defendants have a fiduciary duty to act for the benefit of J&B upon matters within the scope of its relationship with J&B – in particular, to keep its claims processing and revenue cycle service materials secure.

110. Defendants breached their fiduciary duties to Policyholders by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

111. Defendants breached their fiduciary duties to J&B by failing to encrypt and otherwise protect the integrity of the systems containing J&B's claims processing and revenue cycle service materials.

112. Defendants breached their fiduciary duties to J&B when it pulled the plug on the services upon which J&B relied.

113. Defendants breached their fiduciary duties to J&B when they failed to timely notify and/or warn J&B of the Data Breach and its intent to completely disconnect its system.

114. As a direct and proximate result of Defendants' breaches of their fiduciary duties,

J&B has suffered and will continue to suffer injuries.

115. Travelers has paid J&B's insurance claim based on Defendants' actions and now seek reimbursement for such actions. Travelers will have to pay additional insurance claims on behalf of other policyholders because of Defendants' actions.

COUNT VI – DECLARATORY JUDGMENT
(Against All Defendants)

116. Travelers hereby restates the averments contained in the foregoing paragraphs of this complaint as if fully set forth herein.

117. Under the Declaratory Judgement Act, 28 U.S.C. §§ 2201, *et. seq*., this Court is authorized to enter a judgment declaring the rights and legal relation of the parties and grant further necessary relief. Furthermore, this Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal described above.

118. An actual controversy has arisen in wake of the Data Breach at issue regarding Defendants' common law and other duties to act reasonably with respect to safeguarding its systems so that J&B could utilize its services. Travelers, as subrogee and assignee of J&B, alleges that Defendants' actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, J&B continues to suffer injury due to the continued and ongoing threat of additional delays and disruptions of its business and healthcare services to its patients.

119. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, *inter alia*, the following:

a. Defendants owed, and continues to owe, a legal duty to provide accurate and timely payments services for J&B to submit claims and be paid;

b. Defendants' failure to properly secure their computer systems has caused J&B's processing and payment of health claims to halt, disrupting its business operations;

c. Defendants owed, and continues to owe, a legal duty to secure the sensitive information with which they are entrusted, and to notify J&B and its customers of the Data Breach under common law, HIPAA, and Section 5 of the FTC Act;

d. Defendants breached, and continues to breach, their legal duty by failing to employ reasonable measures to secure J&B and its customers' personal and financial information; and

e. Defendants' breach of their legal duties continues to cause harm to J&B.

120. This Court should also issue corresponding injunctive relief requiring Defendants to employ adequate security protocols consistent with industry standards to protect J&B's data.

121. If an injunction is not issued, J&B will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendants' data system. If another breach of Defendants' data system occurs, J&B will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full, and J&B will be forced to bring multiple lawsuits to rectify the same conduct. Monetary damages, while warranted to compensate J&B for its out-of-pocket expenses and other damages that are legally quantifiable and provable, do not cover the full extent of the injuries suffered by J&B.

122. The hardship to J&B if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. J&B will likely be subjected to further monetary harm and other damages. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants has a pre-existing legal obligation to employ such measures.

123. Issuance of the requested injunction will not disserve the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating injuries that resulted to J&B and the public at large.

COUNT VII – UNJUST ENRICHMENT
(Against Change Healthcare)

124. Travelers hereby restates the averments contained in the foregoing paragraphs of this complaint as if fully set forth herein.

125. Travelers brings this count in the alternative to its legal claims and lacks an adequate remedy at law.

126. Upon information and belief, Change funds its data-security measures entirely from their general revenue, including payments made by or on behalf of J&B.

127. As such, a portion of the payments made by or on behalf of J&B is to be used to provide a reasonable level of data security, and the amount of each payment allocated to data security is known to Defendants.

128. J&B conferred a monetary benefit on Change by paying money for services rendered. Specifically, they purchased goods and services from Change and/or their agents and provided Defendants with their claims processing and revenue cycle service materials. In exchange, J&B should have received from Change the goods and services that were the subject

of the transaction and have their processing and service materials protected with adequate data security.

129. Change appreciated and knew that J&B conferred a benefit which Change accepted. Defendants profited from these transactions and used the claims processing and revenue cycle service materials of Policyholders for business purposes.

130. In exchange for receiving J&B's money, thereby providing Change with a commercial benefit, Change was obligated to supply J&B with access to and use of its payment processing and other services. Change reneged on its obligation when it deactivated those services in response to the Data Breach.

131. Change was aware or should have been aware that reasonable consumers would have wanted the services that they had paid for provided and would not have contracted with Change, directly or indirectly, had they known that Change's services and systems were substandard.

132. Change was also aware of the substandard condition of and vulnerabilities in its information systems, and knew that of said condition and vulnerabilities were disclosed, then they would negatively affect J&B's decision to seek goods and/or services therefrom.

133. Change failed to disclose facts pertaining to its substandard information systems relating to defects, vulnerabilities, and the fact that the entire system could be shut down as a result of being substandard before J&B made its decision to make purchases, engage in commerce therewith and seek goods and/or services or information. Instead, Change concealed such information. By concealing that information, Change denied J&B the ability to make rational and informed purchasing decisions and took undue advantage of J&B.

134. Change enriched themselves by saving the costs it reasonably should have

expended in data-security measures to secure J&B' claims processing materials. Instead of providing a reasonable level of security that would have prevented the hacking incident, Change instead calculated to increase their own profits at the expense of J&Bs.

135. Equity and good conscious forbid retention by Change of the financial benefits it obtained from J&B under these circumstances.

136. Change was unjustly enriched at the expense of J&B. Change received profits, benefits, and compensation, in part, at the expense of J&B. By contrast, J&B did not receive the benefit of its bargain because it paid for services that did not satisfy the purpose for which it bought them.

137. Since Change's profits, benefits, and other compensation were obtained by improper means, Change is not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

138. As a result of Change's wrongful conduct, Travelers, as subrogee and assignee of J&B, seeks an Order of this Court requiring Change to refund, disgorge and pay as restitution any profits, benefits, and other compensation obtained by Change from its wrongful conduct and/or the establishment of a constructive trust from which Travelers may seek restitution.

DEMAND FOR A TRIAL BY JURY

Travelers respectfully requests a trial by jury for all claims and issues in its Complaint to which it is or may be entitled to a trial by jury.

PRAYER FOR RELIEF

WHEREAS, PREMISES CONSIDERED, Travelers prays for the following relief:

a. For an Order finding in favor of Travelers as subrogee and assignee of J&B on all counts asserted herein.

b. For damages, including lost profits, actual, nominal, and consequential damages, as allowed by law in an amount to be determined by the trier of fact;

c. Declaratory and injunctive relief as described herein;

d. Awarding Travelers's reasonable attorney's fees, costs, and expenses;

e. Awarding pre- and post-judgment interest on any amount awarded; and

f. For all other Orders, findings, and determinations identified and sought in this Complaint.

g. Awarding such other and further relief as may be just and proper.

This 20th day of February, 2025.

Respectfully submitted,

/s/ Jeffrey S. Price

Jeffrey S. Price (Bar #019550)
MANIER & HEROD, P.C.
1201 Demonbreun St., Ste. 900
Nashville, TN 37203
(615) 742-9358 (phone)
(615) 242-4203 (fax)
jprice@manierherod.com
Attorney for Travelers Casualty and Surety Company of America